

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/389,819	09/03/1999	GREG B. GARRISON	192304-1035	5925

24504 7590 07/23/2004

THOMAS, KAYDEN, HORSTEMEYER & RISLEY, LLP  
100 GALLERIA PARKWAY, NW  
STE 1750  
ATLANTA, GA 30339-5948

EXAMINER
----------

KLIMACH, PAULA W

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 07/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/389,819

Applicant(s)

GARRISON, GREG B.

Examiner

Paula W Klimach

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 19 April 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-36 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-17 and 19-36 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## **DETAILED ACTION**

### ***Response to Amendment***

This office action is in response to amendment filed on 04/19/2004. Original application contained Claims 1-36. Applicant added Claims 31-36. The amendment filed on 04/19/2004 have been entered and made of record. Therefore, presently pending claims are 1-36.

### ***Response to Arguments***

Applicant's arguments filed 04/19/2004 have been fully considered but they are not persuasive because of following reasons.

In reference to claim 1, applicant argued that there is nothing in the cited art to indicate that such a theoretical merged computer would be "configured to receive said...data message," "decrypt said header," and "decrypt said data based on...said header," as claimed in claim 1. In particular, it appears that the UPC, not the theoretical merged computer would decrypt the alleged "data portion." Accordingly, it does not appear that Kaplan discloses, "a second computer configured to decrypt both a header and a data portion of the same data "data message"". This is not found persuasive. The second computer corresponds to the user's PC (UPC) in the system of Kaplan. The UPC buys the cryptolope and therefore receives it from the RCC, which decrypts the key records using its private master key and re-encrypting the document keys (record keys) using the public key of the user's DRWM, this cryptolopes is then processed by the user's viewer (Buying a Cryptolope parts 5-8). The master key is used to encrypt the key record (Cryptolope a cryptographic envelope) with are in turn used to encrypt the documents. The section containing the key record performs the function of the header. As a result, the UPC viewer processes the cryptolope by decrypting using the public key of the user's

DRWM module and then decrypts the encrypted part. The theoretic merged computer would perform the task, as disclosed in claim 1, of "a first computer configured to transmit a data message, said data message having a header and a data portion, said first computer configured to encrypt said data portion via a first encryption technique and to encrypt said header via a second encryption technique, said first computer further configured to include information associated with said first encryption technique in said header."

Applicants clearly have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts. The examiner will not interpret to read narrowly the claim language to read exactly from the specification, but will interpret the claim language in the broadest reasonable interpretation in view of the specification. Therefore, the examiner asserts that Kaplan does teach or suggest the subject matter broadly recited in independent Claims 1, 11, 12, and 30. Dependent Claims 2-10, and 13-29 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action. Accordingly, rejections for claims 1-30 are respectfully maintained.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**Claims 1-4, 11, 12, 14-19, 30, and 31-36** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kaplan.

1. *In reference to claim 1, 11, 12, 31, and 34*, Kaplan discloses a system for securely transmitting data messages, the publisher/ Content creator of page 6 paragraph 1, where a first computer is configured to transmit a data message, the data message having a header and a data portion, and the first computer is configured to encrypt the data portion via a first encryption technique, and to encrypt the header via a second encryption technique, page 3 paragraph 3, the first computer is further configured to include information associated with the first encryption technique in the header, page 5 paragraph 5; and a second computer configured to receive the first data message and to decrypt the header, the second computer, content user/consumer, is further configured to decrypt the data portion based on the information included in the header, page 7 paragraph 1 in combination with paragraph 3.

Kaplan does not expressly disclose a system consisting of two computers.

However, it is obvious that the Publisher and the Royalty Clearing Center could consist of one computer. Kaplan discloses the Publisher and the Royalty Clearing Center as two elements that carry out the key distribution and the encryption of data. These two elements can be carried out in software that is installed on one computer. It would be obvious to one of ordinary skill in the art to carry out the functionality of the Publisher and the Royalty Clearing Center on one computer because this would reduce the cost of another computer especially in a one to one relationship between the Publisher and the Royalty Clearing Center.

*In reference to claim 30*, a method of receiving at a client (UPC) a data packet transmitted from a server (RCC and Publisher: page 6 paragraph 1) that is remotely located from said client, said data packet having a second portion encrypted via a second encryption technique page 3 paragraph 3, said second portion comprising information associated with said first

encryption technique. The information associated with the first encryption technique is the encrypted part that is encrypted with the key record and therefore the encrypted part (the first portion) is associated with the key record (the second portion) that is used to encrypt it. The key record (the second portion) is decrypted using the UPC public encryption key to recover the information. The client decrypts the first portion (encrypted part) using the Record key (section Key records page 3 paragraph 3).

The system of Kaplan does not disclose one server.

However, it is obvious that the Publisher and the Royalty Clearing Center could consist of one computer. Kaplan discloses the Publisher and the Royalty Clearing Center as two elements that carry out the key distribution and the encryption of data. These two elements can be carried out in software that is installed on one computer.

It would be obvious to one of ordinary skill in the art to carry out the functionality of the Publisher and the Royalty Clearing Center on one computer because this would reduce the cost of another computer especially in a one to one relationship between the Publisher and the Royalty Clearing Center.

*In reference to claims 32 and 35*, wherein said first computer randomly selects a first encryption technique for encrypting said data transmitted to said second computer. Keys used for encryption are random numbers and are therefore selected randomly (page 3 paragraph 3).

*In reference to claims 33 and 36*, wherein said second computer is further configured to transmit a list of encryption techniques compatible with said second computer to said first computer (Cryptolope-a cryptographic envelope: page 2 paragraph 2). The controlled access of cryptolopes is basically a key exchange; therefore, the keys are transmitted to the second

computer. The security of the system is based on the security of the keys; therefore the keys perform the function of the encryption techniques. As a result, transporting the keys is equivalent to transporting the techniques.

*In reference to claim 2*, the information associated with the first encryption technique identifies the second encryption technique, page 5 paragraph 5.

*In reference to claims 3 and 14*, the second encryption technique includes RSA encryption, page 3 paragraph 6.

*In reference to claims 4 and 15*, the first encryption technique includes DES encryption, page 3 paragraph 3.

*In reference to claim 16*, Kaplan encrypts the data portion of the first data message with an encryption key and includes the encryption key in said header of said first data message, page paragraphs 3 and 4.

*In reference to claim 17*, the encryption key is selected randomly, page 3 paragraph 3.

*In reference to claim 18*, Kaplan discloses receiving the first data message transmitted in the transmitting step; decrypting the header of the first data message; and decrypting the data portion of the first data message based on said information included in said header of the first data message, page 7 paragraph 3.

*In reference to claim 19*, identify the first encryption technique via information included in the header of the first data message, page 7 paragraph 3.

*In reference to claim 25*, wherein said data message comprises a single data packet, wherein said data portion and said header are contained in said data packet (Figure of cryptolope).



*In reference to claims 26- 28, wherein said information included in said header comprises decryption instructions for decrypting said data portion. The figure of the cryptolope suggests that the information is provided in the same data message and therefore it is obvious that the encryption data can be moved to the header information.*

*In reference to claim 29, wherein said information identifies a key stored at said second computer, and wherein said second computer is configured to select said key based on said information and to use key to decrypt said data portion. The key record disclosed in the figure of the Cryptolope discloses a encrypted key is stored in the key record, therefore it is used by the second computer, the UPC, to decrypt that Encrypted data (paragraph: Key records).*

2. **Claims 5, 7, 8, and 20** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kaplan as applied to claim 1 above, and further in view of Xiao (6,571,337 B1).

*In reference to claims 5 and 20, Kaplan does not expressly disclose the first computer transmits a public key to said second computer.*

Xiao, discloses the first computer transmits a public key to said second computer, claim 6 lines 13-17.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to transmit the key to decrypt the header information of Kaplan with the key of Xiao. One of ordinary skill in the art would have been motivated to do this because the key would be provided after the customer satisfies the terms and conditions for accessing the data entity, Xiao claim 6 lines 9-12.

*In reference to claim 7, Kaplan discloses the structure that is contains the first*

Art Unit: 2135

encryption technique identifies an encryption key used by said first computer to encrypt said data portion, page 3 paragraph 4-7.

*In reference to claim 8*, Xiao discloses a first computer randomly selects said encryption key, column 4 lines 45-47.

3. **Claims 6 and 21** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kaplan and Xiao as applied to claim 5 above, and further in view of Schneier.

Kaplan and Xiao do not expressly disclose first computer is configured to encrypt said public key before transmitting said public key to said second computer.

Schneier discloses an encrypted key exchange, where part of the process is to encrypt the key that is sent, page 518 paragraph 4.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to encrypt the key sent to the consumer in Kaplan using the method of Schneier. One of ordinary skill in the art would have been motivated to do this because it would prevent a third party guessing the key, page 519 paragraph 1.

4. **Claims 9, 10, 13, and 22-24** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kaplan as applied to claim 1 above, and further in view of Leppek (6,233,338 B1).

*In reference to claims 9 and 22*, Kaplan does not disclose transmitting a list of encryption techniques to said first computer and said first computer is configured to select said first encryption technique from said list.

Leppek discloses transmitting a plurality of different operators, claim 1 lines 9-13. This is the equivalent to transmitting the techniques because the operator dictates how the data will be operated on and therefore the technique of encryption.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to transmit the operators from the publisher of Kaplan to the content user of Kaplan, as disclosed in Leppek. One of ordinary skill in the art would have been motivated to do this because a scrambled data stream with no readily discernible encryption footprint will result, column 2 lines 25-40.

*In reference to claim 10, 13, 23, and 24*, the of operators disclosed by Leppek, may vary as required by the user, column 2 lines 51-57, and thus are randomly selected, resulting in random encryption algorithms being created each time.

### ***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

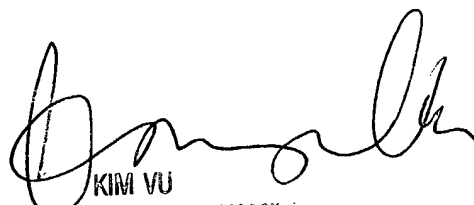
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W Klimach whose telephone number is (703) 305-8421. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

Art Unit: 2135

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK  
Monday, July 12, 2004



KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100